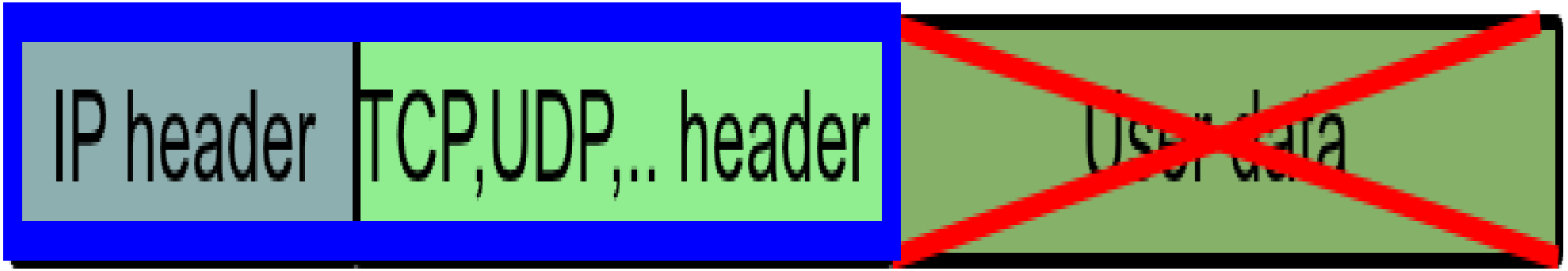
Anonymita na úrovni komunikace ?!?!!!???

- **Internet ~ IP síť**
  - síť na bázi přepínání paketů
- **Paket ~ přenášený datový blok**
  - Nese veškeré informace nutné k doručení na cílové místo
  - Nese informace identifikující zdrojové místo přenosu

Plošné sledování IP provozu sítě

- Tzv. sledování provozu na bázi IP toků (Flow-based monitoring ~ “NetFlow“)
- Informace z hlaviček transportních protokolů (TCP/IP)
- Přijatelný kompromis z hlediska
  - Zachování soukromí koncových uživatelů
  - Dostatečné vypovídací hodnoty o IP provozu
  - Množství dat ke zpracování
  - Možnosti plošného zpracování v rozsáhlých sítích

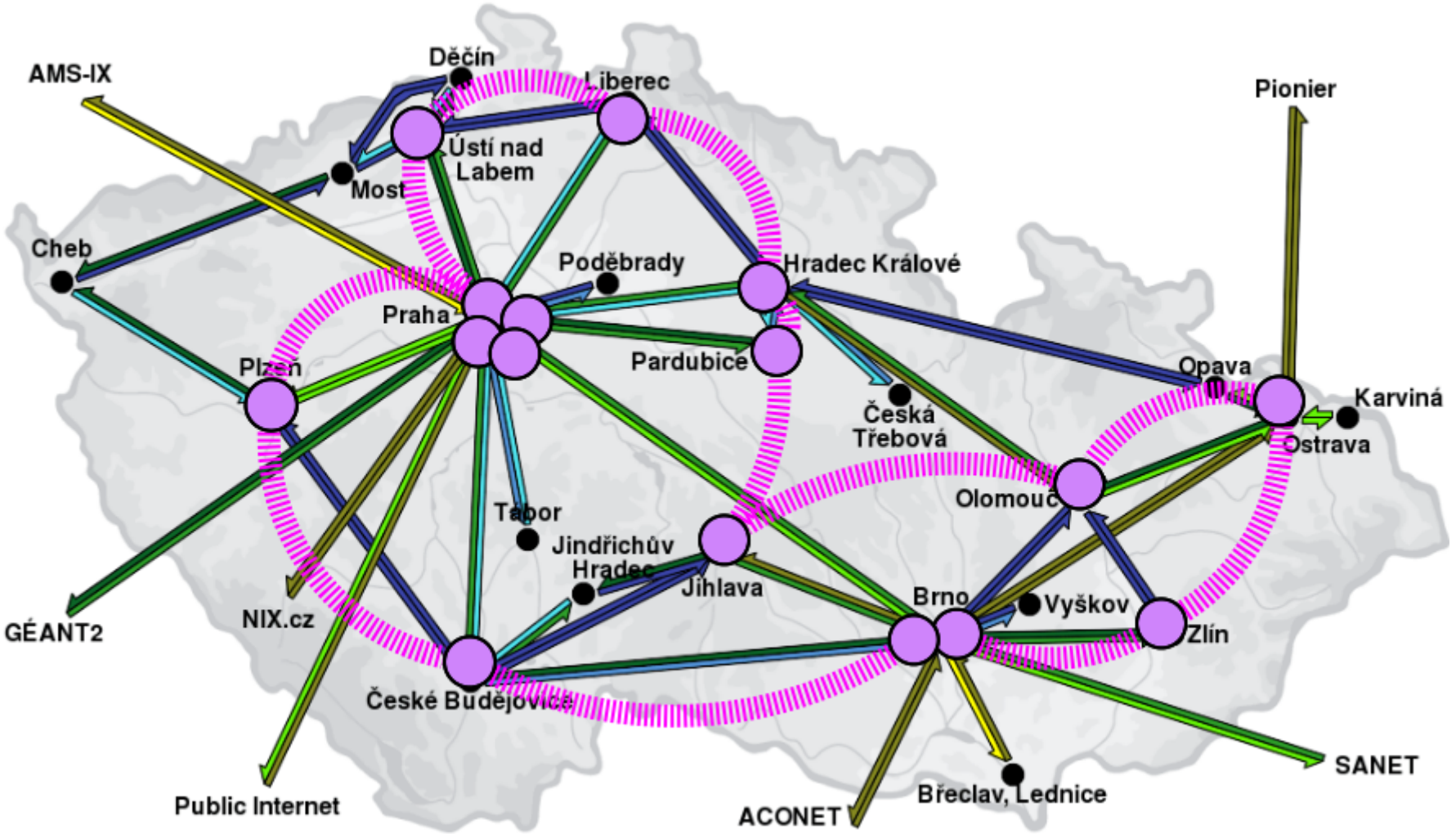


Plošné sledování IP provozu sítě

- Zdroje informací
  - Směrovače, sondy (tj. místa, přes které teče provoz)
- Zpracování informací
  - Tzv. kolektory (zdroje k nim zachycené informace exportují pro další zpracování)
- Typická informační hodnota záznamu o IP provozu
  - Identifikátory toku: IP adresy (zdroj, cíl), protokol (tcp,udp,..), čísla portů služeb, příští IP uzel v cestě a další v závislosti na zdroji (čísla AS, identifikátory rozhraní,..)
  - Objemové ukazatele: počet Bytů, paketů, rozsah v čase
  - Atributy toku: TCP vlaječky, DSCP bity

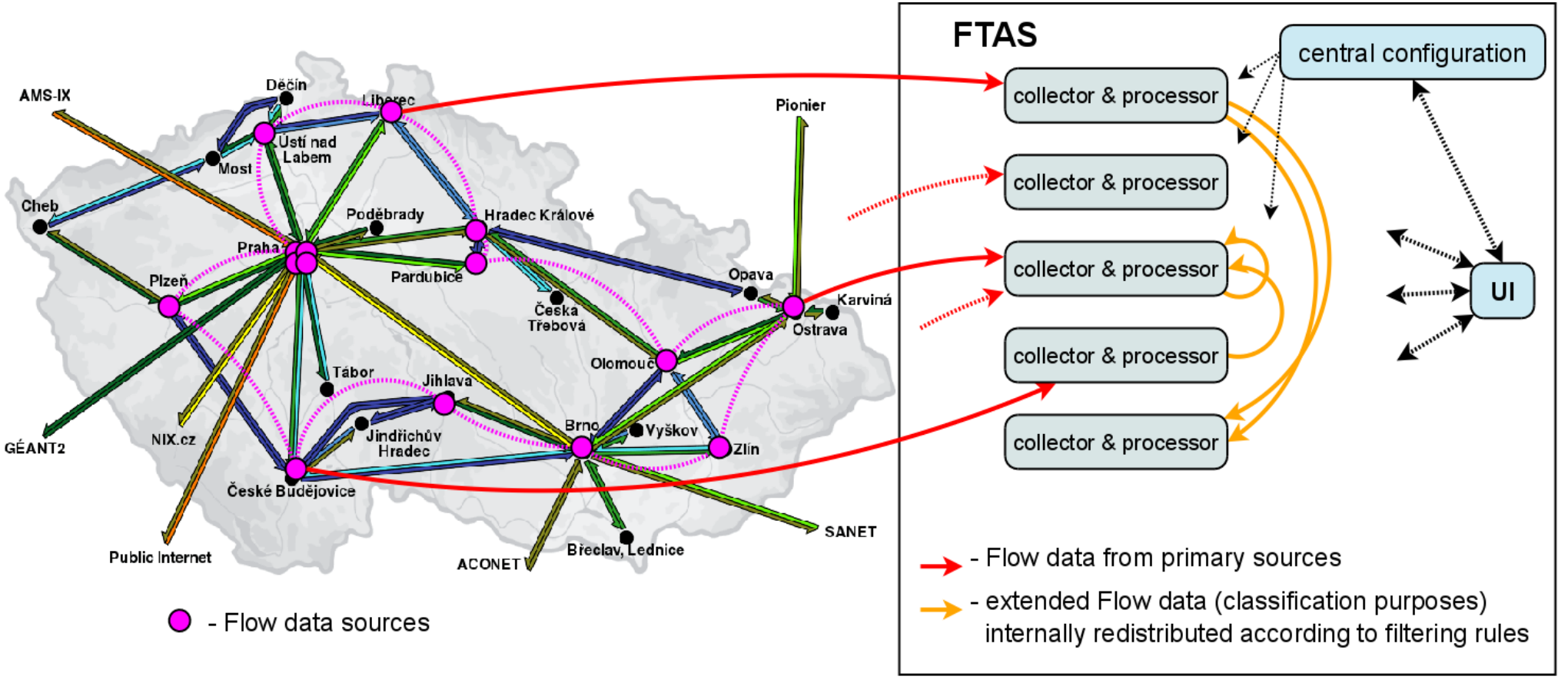
Pokrytí síťové části VI CESNET

- Zdroje informací – páteřní směrovače a HW FlowMon sondy
- Základní a výchozí topologie souvislého sběru provozních informací - hrana IP/MPLS páteřní sítě



Systém FTAS

- Zpracování a zprostředkování informací o provozu pomocí systému **FTAS** (vývoj na CESNETu)
  - Distribuovaný systém, škálovatelný podle objemu příchozích dat a nároků na granularitu zpracování, podpora IPv6, IPv4



Systém FTAS – příklady použití

- Vyhledání rozsahu detekované anomálie ~ útoku

Results *(time values in CEST)*

	Src-IP	Dst-IP	Pkts-measured	Bytes-measured	Flow-Start [CEST]	Flow-End [CEST]	Src-Port	Dst-Port	TCP-flags
1.	112.216.95.35 (KR)	147.x.x.x (CZ)	2.000 p	112.000 B	11/10/20 13:56:25.519	11/10/20 13:56:31.229	53417	ssh (22)	fin(1), syn(2), ack
2.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:59:16.605	11/10/20 13:59:16.605	49316	ssh (22)	syn(2)
3.	112.216.95.35 (KR)	147.x.x.x (CZ)	3.000 p	0.211 KB	11/10/20 13:52:36.806	11/10/20 13:52:42.407	40597	ssh (22)	fin(1), syn(2), pus
4.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:56:16.856	11/10/20 13:56:16.856	47276	ssh (22)	syn(2)
5.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:52:32.221	11/10/20 13:52:32.221	39748	ssh (22)	syn(2)
6.	112.216.95.35 (KR)	147.x.x.x (CZ)	2.000 p	132.000 B	11/10/20 13:56:07.690	11/10/20 13:56:08.626	47220	ssh (22)	syn(2), push(8),
7.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:58:07.385	11/10/20 13:58:07.385	57716	ssh (22)	syn(2)
8.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:54:20.415	11/10/20 13:54:20.415	58499	ssh (22)	syn(2)
9.	112.216.95.35 (KR)	147.x.x.x (CZ)	2.000 p	0.250 KB	11/10/20 13:57:17.768	11/10/20 13:57:19.652	49856	ssh (22)	syn(2), push(8),
10.	112.216.95.35 (KR)	147.x.x.x (CZ)	2.000 p	132.000 B	11/10/20 13:54:25.691	11/10/20 13:54:26.540	59380	ssh (22)	syn(2), push(8),
11.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:58:55.162	11/10/20 13:58:55.162	43045	ssh (22)	syn(2)
12.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:56:29.130	11/10/20 13:56:29.130	33301	ssh (22)	syn(2)
13.	112.216.95.35 (KR)	147.x.x.x (CZ)	3.000 p	0.227 KB	11/10/20 13:54:18.225	11/10/20 13:54:20.388	50534	ssh (22)	syn(2), push(8),
14.	112.216.95.35 (KR)	147.x.x.x (CZ)	3.000 p	0.242 KB	11/10/20 13:53:27.664	11/10/20 13:53:30.827	42458	ssh (22)	syn(2), push(8),
15.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:57:29.759	11/10/20 13:57:29.759	43444	ssh (22)	syn(2)
16.	112.216.95.35 (KR)	147.x.x.x (CZ)	2.000 p	112.000 B	11/10/20 13:53:07.306	11/10/20 13:53:10.157	39326	ssh (22)	fin(1), syn(2), ack
17.	112.216.95.35 (KR)	147.x.x.x (CZ)	2.000 p	164.000 B	11/10/20 13:58:20.025	11/10/20 13:58:22.896	51469	ssh (22)	syn(2), push(8),
18.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:51:43.861	11/10/20 13:51:43.861	55631	ssh (22)	syn(2)
19.	112.216.95.35 (KR)	147.x.x.x (CZ)	3.000 p	0.359 KB	11/10/20 13:52:17.653	11/10/20 13:52:20.425	59659	ssh (22)	syn(2), push(8),
20.	112.216.95.35 (KR)	147.x.x.x (CZ)	2.000 p	112.000 B	11/10/20 13:56:03.644	11/10/20 13:56:06.738	39011	ssh (22)	syn(2), ack(16)
21.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:57:41.552	11/10/20 13:57:41.552	45207	ssh (22)	syn(2)
22.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:55:06.897	11/10/20 13:55:06.897	57446	ssh (22)	syn(2)
23.	112.216.95.35 (KR)	147.x.x.x (CZ)	2.000 p	132.000 B	11/10/20 13:54:10.495	11/10/20 13:54:11.719	48534	ssh (22)	syn(2), push(8),
24.	112.216.95.35 (KR)	147.x.x.x (CZ)	4.000 p	0.277 KB	11/10/20 13:53:00.960	11/10/20 13:53:06.964	37575	ssh (22)	fin(1), syn(2), pus
25.	112.216.95.35 (KR)	147.x.x.x (CZ)	2.000 p	164.000 B	11/10/20 13:51:44.969	11/10/20 13:51:50.615	40204	ssh (22)	syn(2), push(8),
26.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:52:41.550	11/10/20 13:52:41.550	57325	ssh (22)	syn(2)
27.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:57:06.132	11/10/20 13:57:06.132	52254	ssh (22)	syn(2)
28.	112.216.95.35 (KR)	147.x.x.x (CZ)	2.000 p	112.000 B	11/10/20 13:54:42.152	11/10/20 13:54:43.201	48407	ssh (22)	syn(2), ack(16)
29.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:53:03.367	11/10/20 13:53:03.367	60940	ssh (22)	syn(2)
30.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:55:22.316	11/10/20 13:55:22.316	54717	ssh (22)	syn(2)
31.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:55:03.947	11/10/20 13:55:03.947	51880	ssh (22)	syn(2)
32.	112.216.95.35 (KR)	147.x.x.x (CZ)	2.000 p	128.000 B	11/10/20 13:55:23.001	11/10/20 13:55:25.831	38234	ssh (22)	syn(2), push(8),
33.	112.216.95.35 (KR)	147.x.x.x (CZ)	2.000 p	112.000 B	11/10/20 13:55:07.162	11/10/20 13:55:11.814	35649	ssh (22)	syn(2), ack(16)
34.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:57:28.120	11/10/20 13:57:28.120	37020	ssh (22)	syn(2)
35.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:55:31.015	11/10/20 13:55:31.015	39538	ssh (22)	syn(2)
36.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:58:01.168	11/10/20 13:58:01.168	48900	ssh (22)	syn(2)
37.	112.216.95.35 (KR)	147.x.x.x (CZ)	3.000 p	0.211 KB	11/10/20 13:52:52.627	11/10/20 13:52:57.784	46077	ssh (22)	syn(2), push(8),
38.	112.216.95.35 (KR)	147.x.x.x (CZ)	1.000 p	60.000 B	11/10/20 13:59:11.547	11/10/20 13:59:11.547	60041	ssh (22)	syn(2)

Systém FTAS – příklady použití

- Vyhledání specifické komunikace (tcp protokol a pouze SYN vlaječka, pozn. - provoz ZČU)

o	Src-IP	Dst-IP	Pkts-measured	Bytes-measured	Flow-Start [CET]	Flow-End [CET]	Src-Port	Dst-Port	TCP-flags	Protocol
1.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 06:32:37.104	11/11/07 06:32:37.104	52548	netbios-ssn (139)	syn(2)	tcp (6)
2.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 06:33:37.120	11/11/07 06:33:37.120	52552	netbios-ssn (139)	syn(2)	tcp (6)
3.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 06:34:37.116	11/11/07 06:34:37.116	52556	netbios-ssn (139)	syn(2)	tcp (6)
4.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 06:35:37.144	11/11/07 06:35:37.144	52560	netbios-ssn (139)	syn(2)	tcp (6)
5.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 06:36:37.160	11/11/07 06:36:37.160	52564	netbios-ssn (139)	syn(2)	tcp (6)
6.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 06:38:37.168	11/11/07 06:38:37.168	52572	netbios-ssn (139)	syn(2)	tcp (6)
7.	147.228.52.x	147.228.199.x	2.000 p	120.000 B	11/11/07 06:42:18.100	11/11/07 06:42:21.100	39096	www (80)	syn(2)	tcp (6)
8.	147.228.52.x	147.228.199.x	2.000 p	120.000 B	11/11/07 06:42:18.100	11/11/07 06:42:21.100	60734	www (80)	syn(2)	tcp (6)
9.	147.228.52.x	147.228.199.x	2.000 p	120.000 B	11/11/07 06:42:18.100	11/11/07 06:42:21.100	36804	www (80)	syn(2)	tcp (6)
10.	147.228.52.x	147.228.199.x	2.000 p	120.000 B	11/11/07 06:42:18.108	11/11/07 06:42:21.104	53972	www (80)	syn(2)	tcp (6)
11.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 06:46:37.288	11/11/07 06:46:37.288	52622	netbios-ssn (139)	syn(2)	tcp (6)
12.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 06:54:37.396	11/11/07 06:54:37.396	52678	netbios-ssn (139)	syn(2)	tcp (6)
13.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 06:56:37.420	11/11/07 06:56:37.420	52686	netbios-ssn (139)	syn(2)	tcp (6)
14.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 06:57:37.420	11/11/07 06:57:37.420	52690	netbios-ssn (139)	syn(2)	tcp (6)
15.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 06:58:37.448	11/11/07 06:58:37.448	52694	netbios-ssn (139)	syn(2)	tcp (6)
16.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 07:01:37.488	11/11/07 07:01:37.488	52706	netbios-ssn (139)	syn(2)	tcp (6)
17.	147.228.52.x	147.228.199.x	2.000 p	120.000 B	11/11/07 07:02:18.568	11/11/07 07:02:21.568	43671	www (80)	syn(2)	tcp (6)
18.	147.228.52.x	147.228.199.x	2.000 p	120.000 B	11/11/07 07:02:18.568	11/11/07 07:02:21.568	44242	www (80)	syn(2)	tcp (6)
19.	147.228.52.x	147.228.199.x	1.000 p	60.000 B	11/11/07 07:02:18.572	11/11/07 07:02:18.572	42937	www (80)	syn(2)	tcp (6)
20.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 07:02:37.500	11/11/07 07:02:37.500	52716	netbios-ssn (139)	syn(2)	tcp (6)
21.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 07:06:37.552	11/11/07 07:06:37.552	52736	netbios-ssn (139)	syn(2)	tcp (6)
22.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 07:14:37.652	11/11/07 07:14:37.652	52774	netbios-ssn (139)	syn(2)	tcp (6)
23.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 07:15:37.672	11/11/07 07:15:37.672	52778	netbios-ssn (139)	syn(2)	tcp (6)
24.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 07:17:37.696	11/11/07 07:17:37.696	52786	netbios-ssn (139)	syn(2)	tcp (6)
25.	147.228.52.x	147.228.199.x	2.000 p	120.000 B	11/11/07 07:22:19.428	11/11/07 07:22:22.428	36466	www (80)	syn(2)	tcp (6)
26.	147.228.52.x	147.228.199.x	2.000 p	120.000 B	11/11/07 07:22:19.432	11/11/07 07:22:22.428	33894	www (80)	syn(2)	tcp (6)
27.	147.228.52.x	147.228.199.x	2.000 p	120.000 B	11/11/07 07:22:19.432	11/11/07 07:22:22.428	43790	www (80)	syn(2)	tcp (6)
28.	147.228.52.x	147.228.199.x	1.000 p	60.000 B	11/11/07 07:22:19.456	11/11/07 07:22:19.456	58207	www (80)	syn(2)	tcp (6)
29.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 07:22:37.780	11/11/07 07:22:37.780	52822	netbios-ssn (139)	syn(2)	tcp (6)
30.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 07:24:37.808	11/11/07 07:24:37.808	52834	netbios-ssn (139)	syn(2)	tcp (6)
31.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 07:28:37.856	11/11/07 07:28:37.856	52850	netbios-ssn (139)	syn(2)	tcp (6)
32.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 07:29:37.872	11/11/07 07:29:37.872	52854	netbios-ssn (139)	syn(2)	tcp (6)
33.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 07:33:37.924	11/11/07 07:33:37.924	52877	netbios-ssn (139)	syn(2)	tcp (6)
34.	147.228.190.x	10.254.254.x	1.000 p	52.000 B	11/11/07 07:34:37.920	11/11/07 07:34:37.920	52882	netbios-ssn (139)	syn(2)	tcp (6)

Systém FTAS – příklady použití

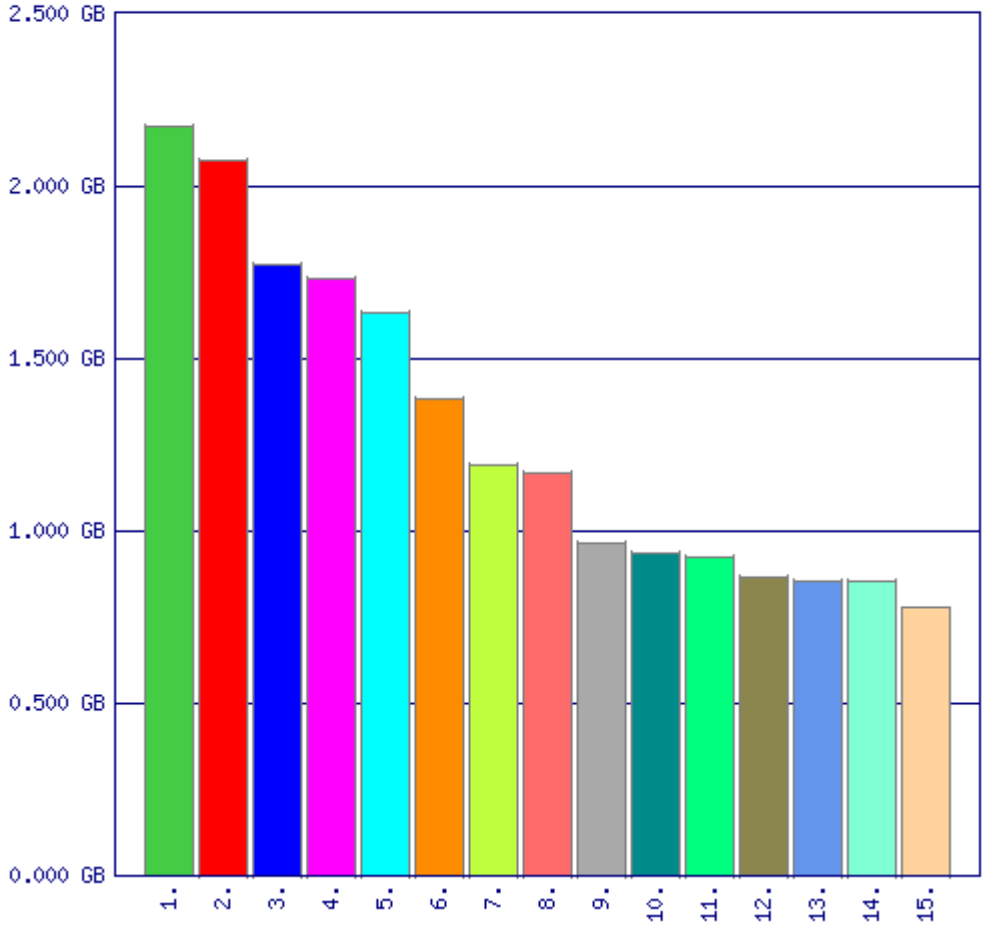
- Vyhledání pravděpodobného významnějšího uzlu v rámci „specifické služby“ – 1. ukázka: top-list bez agregace (výběr pomocí typických rozsahů portů služby)

o	>	Src-IP	Dst-IP	Bytes-estimated	Flow-Start [CET]	Flow-End [CET]	Src-Port	Dst-Port	Protocol
1.		147.228.23.x	78.98.67.x	1.775 GB	11/11/06 14:11:37.671	11/11/06 14:41:59.137	6883	36935	tcp (6)
2.		147.228.23.x	94.112.8.x	1.769 GB	11/11/06 14:41:54.929	11/11/06 15:09:37.137	6883	2587	tcp (6)
3.		78.128.154.x	147.228.23.x	1.730 GB	11/11/06 11:42:28.053	11/11/06 11:54:25.173	59723	6881	tcp (6)
4.		147.228.23.x	217.23.243.x	1.632 GB	11/11/06 18:35:55.453	11/11/06 19:22:31.666	6883	3727	tcp (6)
5.		147.228.23.x	81.30.230.x	1.312 GB	11/11/06 19:47:54.886	11/11/06 21:38:22.330	6883	63193	tcp (6)
6.		147.228.23.x	178.17.80.x	1.166 GB	11/11/06 16:49:16.706	11/11/06 17:06:08.417	6883	1804	tcp (6)
7.		147.228.23.x	91.148.15.x	1.065 GB	11/11/06 21:21:08.868	11/11/06 21:43:50.124	6883	62230	tcp (6)
8.		147.228.23.x	93.91.243.x	0.937 GB	11/11/06 18:43:31.186	11/11/06 19:52:48.336	6883	55673	tcp (6)
9.		147.228.23.x	213.192.60.x	0.921 GB	11/11/06 18:30:36.956	11/11/06 19:02:41.628	6883	62215	tcp (6)
10.		147.228.23.x	217.11.224.x	0.867 GB	11/11/07 07:20:32.256	11/11/07 07:34:30.971	6883	12754	tcp (6)
11.		147.228.23.x	188.112.127.x	0.855 GB	11/11/07 00:03:02.356	11/11/07 00:12:20.052	6883	49691	tcp (6)
12.		147.228.23.x	83.240.113.x	0.851 GB	11/11/06 13:49:18.258	11/11/06 14:55:35.051	6883	1343	tcp (6)
13.		147.228.23.x	78.102.139.x	0.781 GB	11/11/06 19:08:40.061	11/11/06 19:32:15.980	6883	28853	tcp (6)
14.		147.228.23.x	95.103.201.x	0.754 GB	11/11/06 14:22:41.850	11/11/06 15:26:40.872	6883	26474	tcp (6)
15.		195.39.83.x	147.228.23.x	0.727 GB	11/11/06 13:49:22.274	11/11/06 14:41:54.618	56965	6883	tcp (6)
16.		147.228.23.x	90.180.40.x	0.695 GB	11/11/06 15:17:40.966	11/11/06 15:41:22.741	6883	26226	tcp (6)
17.		147.228.23.x	81.201.52.x	0.694 GB	11/11/06 13:15:45.032	11/11/06 13:33:11.752	6881	3448	tcp (6)
18.		147.228.23.x	90.179.20.x	0.663 GB	11/11/06 18:43:43.964	11/11/06 19:24:42.095	6883	51162	tcp (6)
19.		147.228.23.x	195.39.83.x	0.635 GB	11/11/06 14:22:43.111	11/11/06 14:41:57.340	6883	56965	tcp (6)
20.		147.228.23.x	188.167.18.x	0.605 GB	11/11/06 19:41:32.673	11/11/06 20:28:17.098	6883	63621	tcp (6)
21.		213.151.77.x	147.228.23.x	0.545 GB	11/11/06 11:44:35.597	11/11/06 11:54:27.341	56110	6882	tcp (6)
22.		84.114.144.x	147.228.23.x	0.532 GB	11/11/06 13:38:04.531	11/11/06 13:47:20.498	50450	6883	tcp (6)
23.		212.79.105.x	147.228.23.x	0.525 GB	11/11/06 11:47:50.619	11/11/06 12:03:31.481	33193	6881	tcp (6)
24.		147.228.23.x	90.180.40.x	0.501 GB	11/11/06 13:07:52.415	11/11/06 13:15:44.095	6881	22919	tcp (6)
25.		147.228.23.x	178.72.214.x	0.480 GB	11/11/06 15:09:39.203	11/11/06 18:01:04.298	6883	1991	tcp (6)
26.		147.228.23.x	90.180.40.x	0.452 GB	11/11/06 13:50:06.054	11/11/06 14:02:05.862	6881	24146	tcp (6)
27.		147.228.23.x	85.248.44.x	0.412 GB	11/11/06 20:53:49.742	11/11/06 21:01:23.709	6883	52669	tcp (6)
28.		147.228.23.x	90.178.76.x	0.391 GB	11/11/06 13:59:47.488	11/11/06 14:22:39.776	6881	49392	tcp (6)
29.		147.228.23.x	178.72.218.x	0.349 GB	11/11/06 21:21:10.550	11/11/06 21:33:46.454	6883	49704	tcp (6)

Systém FTAS – příklady použití

- Vyhledání pravděpodobného významnějšího uzlu v rámci „specifické služby“ – 2. ukázka – agregát předchozího podle IP-IP, filtr na lokální zdrojové adresy

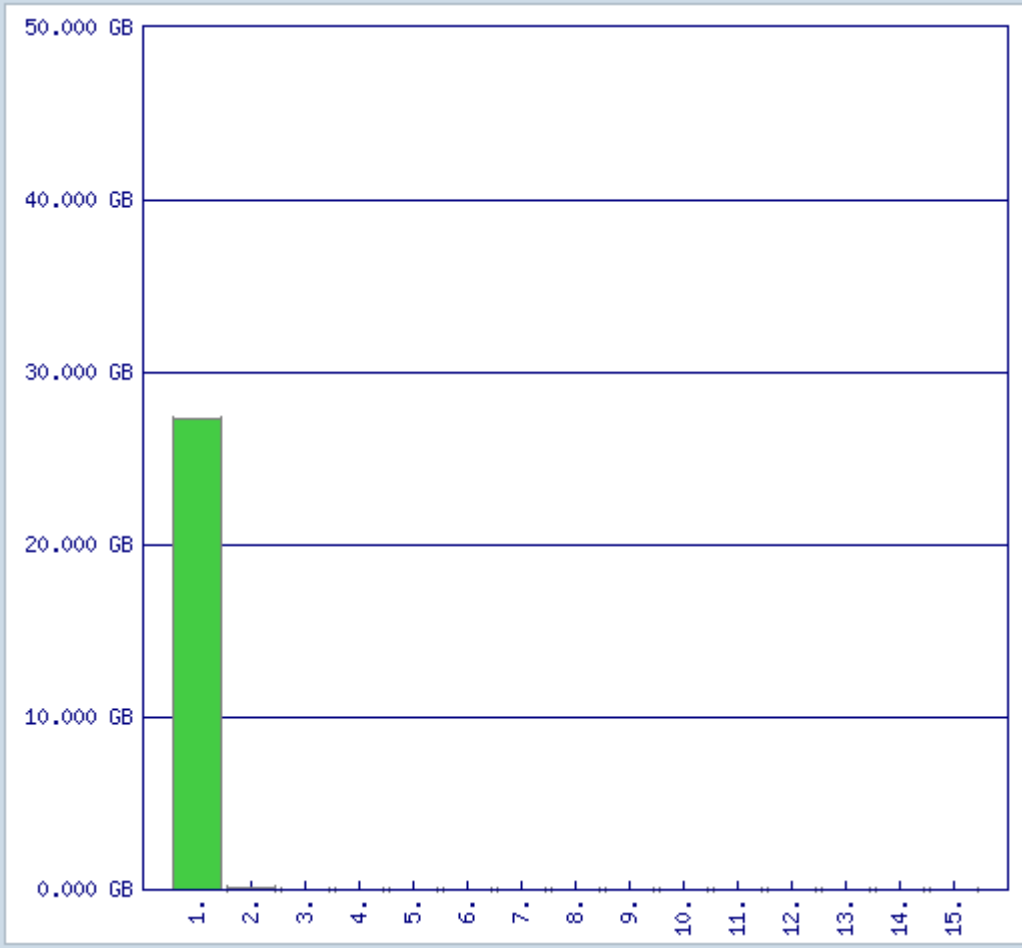
Summary		
In graph	19.291 GB	56.46%
Rest of results	14.874 GB	43.54%
Total	34.165 GB	100.00%



o	>	Src-IP	Dst-IP	Bytes-estimated	Protocol
1.	>	147.228.23.x	90.180.40.x	2.172 GB	tcp (6)
2.	>	147.228.23.x	78.98.67.x	2.075 GB	tcp (6)
3.	>	147.228.23.x	94.112.8.x	1.769 GB	tcp (6)
4.	>	78.128.154.x	147.228.23.x	1.730 GB	tcp (6)
5.	>	147.228.23.x	217.23.243.x	1.632 GB	tcp (6)
6.	>	147.228.23.x	81.30.230.x	1.384 GB	tcp (6)
7.	>	147.228.23.x	91.148.15.x	1.189 GB	tcp (6)
8.	>	147.228.23.x	178.17.80.x	1.166 GB	tcp (6)
9.	>	147.228.23.x	95.103.201.x	0.963 GB	tcp (6)
10.	>	147.228.23.x	93.91.243.x	0.937 GB	tcp (6)
11.	>	147.228.23.x	213.192.60.x	0.921 GB	tcp (6)
12.	>	147.228.23.x	217.11.224.x	0.867 GB	tcp (6)
13.	>	147.228.23.x	188.112.127.x	0.855 GB	tcp (6)
14.	>	147.228.23.x	83.240.113.x	0.851 GB	tcp (6)
15.	>	147.228.23.x	78.102.139.x	0.781 GB	tcp (6)

Systém FTAS – příklady použití

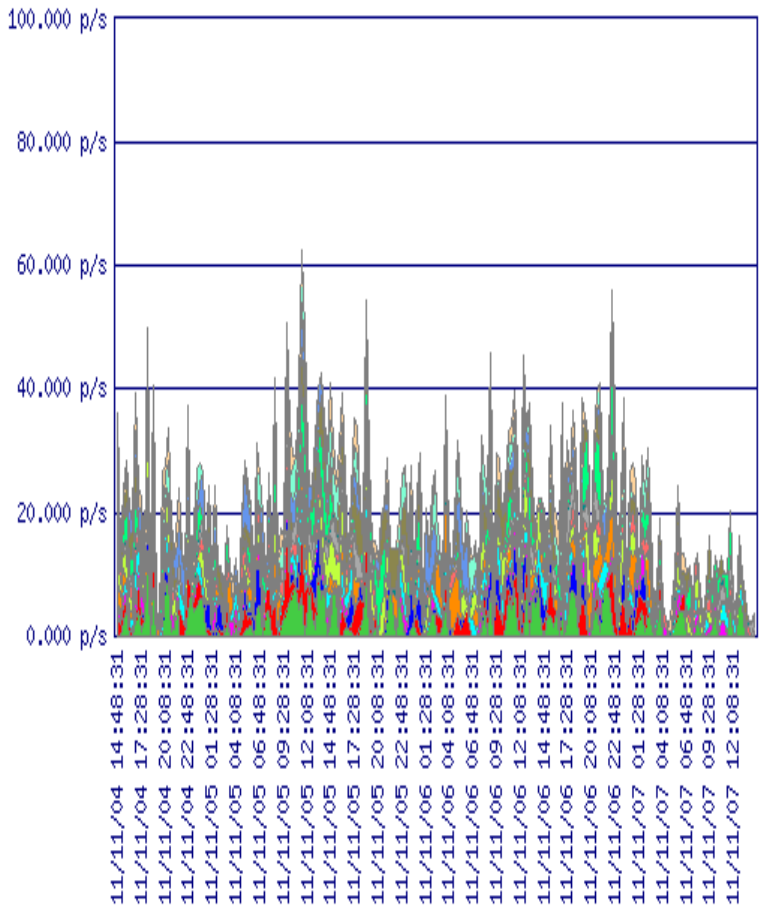
- Vyhledání pravděpodobného významnějšího uzlu v rámci „specifické služby“ – 3. ukázka – pouze zdrojová IP, filtr na lokální zdrojové adresy – výsledek poměrně „signifikantní“



o	Src-IP	Bytes-estimated	Protocol
1.	147.228.23.x	27.349 GB ~ 80.050%	tcp (6)
2.	147.228.209.x	93.415 MB ~ 0.267%	udp (17)
3.	147.228.64.x	28.577 MB ~ 0.082%	tcp (6)
4.	147.228.4.x	11.199 MB ~ 0.032%	tcp (6)
5.	147.228.209.x	11.194 MB ~ 0.032%	udp (17)
6.	147.228.98.x	9.500 MB ~ 0.027%	tcp (6)
7.	147.228.184.x	6.910 MB ~ 0.020%	tcp (6)
8.	147.228.57.x	5.135 MB ~ 0.015%	tcp (6)
9.	147.228.183.x	4.886 MB ~ 0.014%	tcp (6)
10.	147.228.41.x	4.138 MB ~ 0.012%	tcp (6)
11.	147.228.94.x	4.126 MB ~ 0.012%	tcp (6)
12.	147.228.47.x	3.569 MB ~ 0.010%	tcp (6)
13.	147.228.98.x	3.126 MB ~ 0.009%	udp (17)
14.	147.228.209.x	2.687 MB ~ 0.008%	udp (17)
15.	147.228.60.x	2.596 MB ~ 0.007%	tcp (6)

Systém FTAS – příklady použití

- Komunikace uzlu v rámci „specifické služby“ v čase (jiná služba než v předchozí ukázce)



0	Src-IP	Dst-IP	Pkts-estimated	Bytes-estimated	Src-Port	Dst-Port	Protocol
1.	94.198.110.x	147.228.41.x	0.585 mp ~ 8.133%	178.326 MB ~ 15.730%	411	3004	tcp (6)
2.	89.38.249.x	147.228.41.x	0.435 mp ~ 6.053%	143.270 MB ~ 12.638%	411	2422	tcp (6)
3.	190.120.237.x	147.228.41.x	0.322 mp ~ 4.481%	109.645 MB ~ 9.672%	411	1906	tcp (6)
4.	212.117.163.x	147.228.41.x	0.220 mp ~ 3.063%	107.585 MB ~ 9.490%	411	4407	tcp (6)
5.	91.82.85.x	147.228.41.x	0.357 mp ~ 4.962%	98.915 MB ~ 8.725%	411	2036	tcp (6)
6.	178.130.0.x	147.228.41.x	0.359 mp ~ 4.996%	79.814 MB ~ 7.040%	411	4408	tcp (6)
7.	91.121.134.x	147.228.41.x	0.455 mp ~ 6.322%	66.705 MB ~ 5.884%	411	3627	tcp (6)
8.	87.96.239.x	147.228.41.x	0.234 mp ~ 3.246%	61.194 MB ~ 5.398%	411	4869	tcp (6)
9.	195.160.162.x	147.228.41.x	0.310 mp ~ 4.307%	39.228 MB ~ 3.460%	411	3606	tcp (6)
10.	77.36.69.x	147.228.41.x	117.801 kp ~ 1.638%	38.415 MB ~ 3.389%	411	3890	tcp (6)
11.	147.228.41.x	94.198.110.x	0.535 mp ~ 7.430%	24.281 MB ~ 2.142%	3004	411	tcp (6)
12.	147.228.41.x	91.121.134.x	0.542 mp ~ 7.536%	24.214 MB ~ 2.136%	3627	411	tcp (6)
13.	147.228.41.x	178.130.0.x	0.398 mp ~ 5.529%	19.233 MB ~ 1.697%	4408	411	tcp (6)
14.	147.228.41.x	190.120.237.x	0.406 mp ~ 5.648%	19.204 MB ~ 1.694%	1906	411	tcp (6)
15.	147.228.41.x	89.38.249.x	0.394 mp ~ 5.473%	18.284 MB ~ 1.613%	2422	411	tcp (6)

Anonymita na úrovni komunikace ?!?!!!???

- V Internetu nejsme anonymní...

...ani na úrovni prosté IP komunikace...

...stopy každého přenosu v Internetu mohou být zaznamenány a uschovány pro případné řešení konfliktních situací...